RECEIVED
CENTRAL FAX CENTER
SEP 14 2006

AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method for generating an encryption key for use with a host device having a host identification stored therein, for ~~encryption~~ encrypting a file, which comprises ~~comprising~~ a plurality of blocks of plaintext data, in a manner that said encrypted file can only be decrypted by said host device, the method comprising:

retrieving the host identification from the host device for use as a private portion of an encryption key;

generating at least one content variable ~~that uniquely identifies a corresponding block of said file~~ as a public portion of said encryption key, where said at least one content variable uniquely identifies a corresponding block of said file;

combining the host identification and the at least one content variable to produce the encryption key;

encrypting a block of plaintext data using the encryption key to produce a block of ciphertext;

appending only the at least one content variable to the block of ciphertext; and

storing the block of ciphertext and the appended one or more content variable within a storage device.

2. (Previously presented) The encryption key generation method of claim 1 wherein said step of combining comprises:

using a predetermined method, wherein combining the host identification and the at least one content variable repeatedly produces the same encryption key.

3. (Previously presented) The encryption key generation method of claim 1, wherein the host device includes a secure clock, the method further comprising:

obtaining a time variable from the secure clock within the host device;

combining the host identification, the at least one content variable and the time variable to produce the encryption key.

4. (Previously presented) A method for generating an encryption key to encrypt a block of plaintext for use with a host device having a secure clock and a host identification assigned thereto and saved therein, the method comprising:

retrieving the host identification from the host device for use as a private portion of an encryption key;

generating a content identification, wherein the content identification corresponds to the block of plaintext as a public portion of said encryption key;

obtaining a time variable from the secure clock within the host device;

combining the host identification, the content identification and the time variable to produce the encryption key.

5. (Currently Amended) A method for encrypting a block of plaintext for transmission over an unsecured interface to a storage device, for use with a host device having a host identification assigned thereto and stored therein, the method comprising:

retrieving the host identification from the host device for use as a private portion of an encryption key;

generating at least one content variable ~~that uniquely identifies a corresponding block of said file~~ as a public portion of said encryption key, where said at least one content variable uniquely identifies a corresponding block of said file;

combining the host identification and the at least one content variable to produce an encryption key;

encrypting the block of plaintext using the ~~first~~ encryption key to produce a block of ciphertext;

appending the at least one content variable to the block of ciphertext;

transmitting the block of ciphertext and the appended at least one content variable over the unsecured interface to the storage device; and

storing the block of ciphertext and the appended one or more content variables within the storage device.

6. (Previously presented) The method of encrypting the block of plaintext of claim 5, wherein the host device further comprises a secure clock, the method further comprising:

obtaining a first time variable from the secure clock within the host device;

combining the host identification, the at least one content variable and the first time variable to produce an encryption key.

7. (Previously presented) The method of encrypting the block of plaintext of claim 6, for further use decrypting the block of ciphertext, the method comprising:

retrieving the stored block of ciphertext and the appended at least one content variable from the storage device;

retrieving the host identification from the host device;

obtaining a second time variable from the secure clock within the host device;

combining the host identification, the at least one content variable and the second time variable to produce a second encryption key, wherein if the first time variable and the second time variable do not match, the second encryption key will not decrypt the block of ciphertext and if the first time variable matches the second time variable the second encryption key will decipher the block of ciphertext.

8. (Previously presented) The method of encrypting the block of plaintext of claim 5 for further use decrypting the stored block of ciphertext, the method comprising:

retrieving the stored block of ciphertext and the appended at least one content variable from the storage device;

retrieving the host identification from the host device;

combining the host identification and the at least one content variables to produce the encryption key that was used to encrypt the file; and

decrypting the block of ciphertext with the encryption key to produce the block of plaintext.

9. (Previously presented) The encryption key generation method of claim 3 further comprising:

retrieving the stored block of ciphertext and the appended at least one content variable from the storage device;

retrieving the host identification from the host device;

obtaining a second time variable from the secure clock within the host device;

combining the host identification, the at least one content variable, and the second time variable to produce a second encryption key, wherein if the first time variable and the second time variable do not match, the second encryption key will not decrypt the block of ciphertext; and if the first time variable matches the second time variable, the second encryption key will decipher the block of ciphertext.

10. (Previously presented) The encryption key generation method of claim 1 further comprising:

retrieving the stored block of ciphertext and the appended at least one content variable from the storage device;

retrieving the host identification from the host device;

combining the host identification and the at least one content variable to produce the encryption key that was used to encrypt the file; and

decrypting the block of ciphertext with the encryption key to produce the block of plaintext data.

11. (Previously presented) The encryption key generation method of claim 5 wherein said step of combining comprises:

using a predetermined method, wherein combining the host identification and the at least one content variable produces the same encryption key each time the encryption key generation process is executed.